



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/592,916	06/13/2000	Adriano Huber	PM 258042	5750
909	7590	09/23/2005	EXAMINER	
PILLSBURY WINTHROP SHAW PITTMAN, LLP P.O. BOX 10500 MCLEAN, VA 22102			GYORFI, THOMAS A	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 09/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/592,916

Applicant(s)

HUBER ET AL.

Examiner

Tom Gyorfi

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 February 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

12

DETAILED ACTION

1. Claims 1-35 remain for examination. The correspondence filed 2/23/05 amended claims 1, 3, 4, 6, 8, 15, 18-20, and 25.

2. In view of the amendment filed on 2/23/05, PROSECUTION IS HEREBY REOPENED. New grounds for rejection are set forth below.

Response to Arguments

3. Applicant's arguments, see the amendment filed 2/23/05, with respect to the rejection of claim 25 under Gelman have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Gelman and RFC2246.

4. Applicant's arguments with respect to claim 18 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gelman (U.S. Patent 6,415,329), and further in view of RFC2246 ("The TLS Protocol, Version 1.0"; hereinafter "RFC2246").

Regarding claim 25:

Gelman discloses a method by which a terminal can access a server, said method comprising the steps of:

said terminal sending a request for said server to a gateway (col. 10, lines 50-650, wherein security utilized between said terminal and said gateway is based on a first security protocol (col. 11, lines 1-10);

securing said server with a second security protocol, said second security protocol also including an encryption (col. 3, lines 1-5); and

converting between said first and said second security protocol in a secured domain of said server administrated by an administrator (col. 31, lines 50-65; col. 7, lines 15-30), and wherein

encrypted packets sent by said terminal are routed by said gateway to said secured domain without said gateway decrypting all of the packets transmitted during a session (col. 11, lines 1-10).

Although Gelman does not disclose "said first security protocol including an encryption", Gelman does teach that the invention is not limited to converting packets from TCP to WLP, but can alternatively be used as a generic translator between packets of any protocol (col. 31, lines 40-67). RFC2246 discloses a protocol designed

Art Unit: 2135

to operate in conjunction with TCP to add encryption and security to network traffic (page 3, "Introduction"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow conversion between TLS (a first security protocol containing an encryption) to WLP. The motivation for doing so would be to permit the creation of a more flexible firewall that can keep private networks secure (col. 32, lines 14-22).

7. Claims 1-17, 19-24, and 26-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lincke (U.S. Patent 6,253,326), and further in view of "Wireless Authentication Protocol Wireless Transport Layer Specification" (hereinafter, "WAP WTLS").

Referring to Claim 1:

Lincke discloses a method by which a mobile subscriber with a WAP-enabled terminal can access a WEB or WAP server, comprising the steps of:

said terminal sending a request for said server to a WAP gateway (col. 8, lines 40-50), wherein encryption in the wireless interface between said WAP-enabled terminal (col. 83, lines 1-10), and

wherein an encryption protocol used by said server is based on the SSL and/or TLS security protocol (col. 111, lines 15-25); and

converting between [WTLS] and SSL and/or TLS in a secured domain of said server administrated by an administrator (col. 91, lines 50-65), wherein the [WTLS]

Art Unit: 2135

encrypted packets sent by said terminal are routed by said gateway to said secured domain without said gateway decrypting all of the encrypted packets transported during a session (col. 17, lines 40-50; col. 113, line 55-col. 114, line 15).

Although Lincke does not explicitly disclose the use of WTLS, it does provide for the use of alternate wireless protocols (col. 115, lines 35-40). WAP WTLS discloses the use of the WTLS protocol, which is modular and can thus be layered on top of an existing transport layer protocol, and also contains an encryption (Section 1, "Scope"; Section 5.1, "Reference Model"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use WTLS in the invention disclosed by Lincke. The motivation for doing so would be to use a technology that is widely known as an industry standard, rather than the proprietary protocol technology disclosed by Lincke, to facilitate its acceptance (WAP WTLS, Section 1, "Scope", 1st paragraph).

Referring to Claim 2:

Lincke and WAP WTLS disclose the limitations of Claim 1 above. Lincke further discloses said gateway routes said packets to a proxy in said secured domain, said proxy using at least one protocol layer of the WAP protocol (col. 17, lines 40-45; col. 18, lines 45-68).

Referring to Claim 3:

Lincke and WAP WTLS disclose the limitations of Claim 2 above. Lincke further discloses said packets are routed according to the URL and/or the domain name of the requested page in said gateway (col. 114, lines 20-35).

Referring to Claim 4:

Lincke and WAP WTLS disclose the limitations of Claim 2 above. Lincke further discloses said packets are routed according to the port number (col. 114, lines 20-35).

Referring to Claim 5:

Lincke and WAP WTLS disclose the limitations of Claim 4 above. Lincke further discloses said encrypted packets are routed according to different port numbers to different secured domains (col. 18, lines 20-35).

Referring to Claim 6:

Lincke and WAP WTLS disclose the limitations of Claim 4 above. Lincke further discloses said port numbers are extracted in an application layer of said gateway from the URL of the request page (col. 18, lines 20-35).

Referring to Claim 7:

Lincke and WAP WTLS disclose the limitations of Claim 6 above. Lincke further discloses said port number is extracted from only a restricted number packets during a

session, and wherein the routing of at least one of the following packets depends on this extracted port number (col. 17, lines 10-25; col. 18, lines 20-40;).

Referring to Claim 8:

Lincke and WAP WTLS disclose the limitations of Claim 7 above. Lincke further discloses wherein a proxy server in said secured domain extracts the URL and/or the port number of the received packets and where the proxy server sends back a command to said gateway if it receives a packet with a different URL and/or port number (col. 18, lines 20-68).

Referring to Claim 9:

Lincke and WAP WTLS disclose the limitations of Claim 4 above. Lincke further discloses said port number is extracted from said URL of the required web page in said terminal (col. 18, lines 20-30).

Referring to Claim 10.

Lincke and WAP WTLS disclose the limitations of Claim 9 above. Lincke further discloses said port number is extracted by a browser from said URL of the required web page (col. 11, lines 15-40).

Referring to Claim 11:

Lincke and WAP WTLS disclose the limitations of Claim 8 above. Lincke further discloses, wherein the browser in said terminal only copies said port number in said packets if an end-to-end secured connection is requested (col. 13, lines 35-50).

Referring to Claim 12:

Lincke and WAP WTLS disclose the limitations of Claim 3 above. Lincke further discloses said packets in said gateway are routed to a secured domain if said port number is comprised in a predefined range (col. 114, lines 20-30).

Referring to Claim 13:

Lincke and WAP WTLS disclose the limitations of Claim 3 above. Lincke further discloses said gateway sends a redirect command to said terminal if an end-to-end secured connection is requested (col. 18, lines 30-40; col. 19, lines 5-25).

Referring to Claim 14:

Lincke and WAP WTLS disclose the limitations of Claim 13 above. Lincke further discloses said redirect command is time limited (col. 19, lines 1-25).

Referring to Claim 15:

Lincke and WAP WTLS disclose the limitations of Claim 13 above. Lincke further discloses a proxy server in said secured domain extracts the URL and/or the port

number of the received packets and sends a redirect command back to said terminal as soon as the session is to be routed to said gateway (col. 18, lines 35-65; col. 19, lines 1-35).

Referring to Claim 16:

Lincke and WAP WTLS disclose the limitations of Claim 13 above. Lincke further discloses said redirect command contains a forwarding address which is extracted from a document made accessible by said WEB or WAP server (col. 19, lines 1-20).

Referring to Claim 17:

Lincke and WAP WTLS disclose the limitations of Claim 13 above. Lincke further discloses said redirect command contains a document which includes the forwarding address (col. 18, lines 20-65).

Referring to Claim 19:

Lincke discloses a gateway comprising:
means for receiving packets encrypted according to the [WTLS] protocol from WAP-enabled terminals (col. 18, lines 1-20, 60-68);
means for converting said packets into SSL-encrypted requests (col. 91, lines 50-51); and means for transmitting said SSL-requests to a receiving server (col. 91, lines 50-51), wherein said gateway can recognize [WTLS]-encrypted packets that are to be sent on transparently and can convert said [WTLS]-encrypted packets into

SSL-encrypted request without decrypting the information contained in said [WTLS]-encrypted packets (col. 18, lines 1-65; col. 83, lines 1-20; col. 92, lines 10-15).

Although Lincke does not explicitly disclose the use of WTLS, it does provide for the use of alternate wireless protocols (col. 115, lines 35-40). WAP WTLS discloses the use of the WTLS protocol, which is modular and can thus be layered on top of an existing transport layer protocol, and also contains an encryption (Section 1, "Scope"; Section 5.1, "Reference Model"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use WTLS in the invention disclosed by Lincke. The motivation for doing so would be to use a technology that is widely known as an industry standard, rather than the proprietary protocol technology disclosed by Lincke, to facilitate its acceptance (WAP WTLS, Section 1, "Scope", 1st paragraph).

Referring to Claim 20:

Lincke and WAP WTLS disclose the limitations of Claim 19 above. Lincke further discloses wherein said WTLS-encrypted packets are routed according to the URL and/or the domain name of the requested page (col. 114, lines 20-35).

Referring to Claim 21:

Lincke and WAP WTLS disclose the limitations of Claim 19 above. Lincke further discloses said WTLS-encrypted packets are routed according to the port number of the requested page (col. 18, lines 20-45; col. 114, lines 20-35).

Referring to Claim 22:

Lincke and WAP WTLS disclose the limitations of Claim 21 above. Lincke further discloses said WTLS-encrypted packets are routed to different secured domains according to different port numbers (col. 18, lines 20-45).

Referring to Claim 23:

Lincke and WAP WTLS disclose the limitations of Claim 21 above. Lincke further discloses said port number is extracted from the URL of the requested page in an application layer of said gateway (col. 8, lines 5-35).

Referring to Claim 24:

Lincke and WAP WTLS disclose the limitations of Claim 21 above. Lincke further discloses said port number is extracted during a session only from a restricted number of WTLS-encrypted packets, and wherein the routing of at least one following WTLS-encrypted packet depends on said extracted port number (col. 17, lines 10-30; col. 18, lines 20-40).

Referring to Claims 26 and 31:

A method for performing end-to-end secure data transfer between a terminal and a server, wherein said terminal is connected to said server via a wireless connection between said terminal and a gateway, said method comprising the steps of:

said terminal requesting a secure communication session with said server via said gateway, said requesting including the steps of (col. 17, lines 40-50):

said terminal generating a request including request packets encrypted using a [WTLS] protocol (col. 83, lines 1-20), said terminal sending said request to said gateway, said gateway forwarding said request to said server or to another server (col. 18, lines 20-45), wherein said gateway does not decrypt all of said request packets, and said server or said another server decrypting some number of said request packets using said [WTLS] protocol (91, lines 50-60);

and

said server or said another server serving data to said terminal via said gateway, said serving including the steps of:

said server or said another server sending said data including data packets encrypted using said [WTLS] protocol to said gateway (col. 114, line 45-col. 115, line10);

said gateway forwarding said data packets to said terminal, wherein said gateway does not decrypt all of said data packets (col. 18, lines 20-35); and said terminal decrypting said data packets using said WTLS protocol (col. 89, lines 5-20).

Although Lincke does not explicitly disclose the use of WTLS, it does provide for the use of alternate wireless protocols (col. 115, lines 35-40). WAP WTLS discloses the use of the WTLS protocol, which is modular and can thus be layered on top of an existing transport layer protocol, and also contains an encryption (Section 1, "Scope"; Section 5.1, "Reference Model"). It would have been obvious to one of ordinary skill in

the art at the time the invention was made to use WTLS in the invention disclosed by Lincke. The motivation for doing so would be to use a technology that is widely known as an industry standard, rather than the proprietary protocol technology disclosed by Lincke, to facilitate its acceptance (WAP WTLS, Section 1, "Scope", 1st paragraph).

Referring to Claims 27 and 32:

Lincke and WAP WTLS disclose the limitations of Claims 26 and 31 above. Lincke further discloses said gateway must decrypt some but not all of said request packets to forward said request to said server or said another server (col. 18, lines 20-35).

Referring to Claims 28 and 33:

Lincke and WAP WTLS disclose the limitations of Claims 27 and 32 above. Lincke further discloses said gateway must decrypt some but not all of said data packets to forward said data to said terminal (col. 18, lines 45-60).

Referring to Claims 29 and 34:

Lincke and WAP WTLS disclose the limitations of Claims 26 and 32 above. Lincke further discloses a browser on said terminal provides information to said gateway for forwarding said request to said server or said another server without said gateway decrypting any of said request packets (col. 11, lines 25-50).

Referring to Claims 30 and 35:

Lincke and WAP WTLS disclose the limitations of Claims 29 and 34 above.

Lincke further discloses said information includes one or more of: a port number, a domain name, and an URL (col. 18, lines 20-45).

8. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over "WAP Architecture: Wireless Application Protocol Specification" (hereinafter, "WAP1"), "Wireless Application Protocol: Wireless Transaction Protocol Specification" (hereinafter, "WAP2"), and further in view of RFC2068 ("Hypertext Transfer Protocol – HTTP/1.1", hereinafter "RFC2068").

Regarding claim 18:

WAP1 and WAP2 (incorporated by reference to WAP1: see WAP1, "7.3 Wireless Transaction Protocol (WTP)") discloses a method by which a mobile user with a WAP enabled terminal can access a web or WAP server, said method comprising the steps of said terminal sending a request for said server to a WAP gateway using a browser (WAP1, "6.2 The WAP Model") and routing said packets, using said gateway, according to a port number (WAP2, page 14, "5.3 Relation to Other Protocols"; pages 19-20). It should also be noted that the WAP references disclose that WWW standard URLs are used to identify and access content from a WAP browser (WAP1, page 12, "6.2 The WAP Model"; page 16, "Wireless Session Protocol"). RFC2068 discloses the HTTP protocol, including the ability to indicate a port number as part of a URL to route the

packets (RFC2068, page 20). Even if Applicant's argument that this ability was not present in state-of-the-art browsers at the time of the invention (an assertion that Examiner disagrees with), it would have been obvious to one of ordinary skill in the art at the time the invention was made to allow a WAP browser to specify a specific port number as part of the URL for desired content. The motivation for doing so would be to allow for non-standard ports in the event that other transport layer protocols are used, without breaking application layer functionality (RFC2068, page 12, 3rd paragraph).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- "Sendo Licences WAP Browser from Digital Mobility" ©2001 Sendo.
- Khare, Rohit. "W* Effect Considered Harmful". ©1999 4k Associates.
- Bort, Julie. "A WAP on the Head" © 2000 Network World.
- WAP Architecture: Wireless Application Protocol Architecture Specification.
© 1998 Wireless Application Protocol Forum, Ltd.

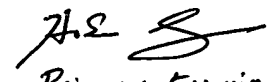
10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

Art Unit: 2135

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
9/12/05


Primary Examiner
Art Unit 2135